Datensicherheit auf höchstem Niveau

Cloudbasierte Lösungen für das Informationsmanagement in der Prozessindustrie bieten erhebliche Vorteile in Bezug auf Erreichbarkeit, Skalierbarkeit, Wartung und Verwaltung. Aber sind solche Lösungen auch sicher genug für die chemische und pharmazeutische Industrie, die eine enorme Menge an hochsensiblen Daten schützen müssen?

Der steigende Bedarf an Anwendungen mit sicherer, schnell skalierbarer Datenspeicherung und -verarbeitung führte zu einer zunehmenden Relevanz von Cloud Computing – der Datenverarbeitung und -speicherung auf einem externen Server. Als Software-as-a-Service-Lösung (SaaS) werden Tools so von einem externen Provider bereitgestellt. Die hauseigene IT muss sich nicht um die IT-Infrastruktur, Updates und das Hosting kümmern. Zur Debatte, ob Cloud oder On-Prem einen höheren Stellenwert hat, tragen die sich schnell wandelnden Anforderungen unter volatilen Marktbedingungen ebenso bei wie die Anforderungen nach reduziertem E-Mail-Verkehr und einer soliden Datenbasis, die sich auch dezentral abrufen lässt, sensible Daten und eine sich ständig wandelnde Gefahrenlandschaft in der IT sowie die steigende Nachfrage nach Services wie KI-basierte Anwendungen.

Noch heute zögern viele Pharmahersteller, ihre Daten in die Cloud zu geben. Doch eine gut konzipierte Cloudlösung, die den modernen Sicherheitsstandards und -vorschriften entspricht, kann tatsächlich sicherer sein als die Speicherung von Daten im eigenen internen Netzwerk. So bieten solche Lösungen zusätzliche Sicherheit durch zentrale Datenspeicherung, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten – vor allem für Unternehmen, die bereits den Schritt in ein digitalisiertes Prozessmanagement gemeistert haben.

Mit einer cloudbasierten Softwarelösung können Schichtteams in der Prozessindustrie effizienter und sicherer arbeiten.
Bild: Depositphotos/iStock

On-Premise vs. Cloud

Bei der Bewertung der Sicherheit einer Softwarelösung sind drei Elemente zu berücksichtigen. Diese Bausteine sind in der Softwarebranche als CIA-Trias bekannt und stehen für Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit). Vertraulichkeit bezieht sich darauf, wie Daten vor Offenlegung oder unbefugtem Zugriff geschützt werden. Wer darf Daten einsehen? Wie wird der Zugriff kontrolliert? Welche Schutzmaßnahmen verhindern, dass Unbefugte in das System eindringen? Bei Integrität geht es darum, wie genau und zuverlässig die Daten sind. Gibt es doppelte Eingaben oder eine unzuverlässige Informationsquelle? Verfügbarkeit bedeutet, dass die Daten zugänglich und nutzbar sind, wann und wo sie gebraucht werden, und dass sie nicht aufgrund von Systemausfällen, Netzwerkfehlern oder anderen Störungen unzugänglich wurden.

In allen drei Bereichen kann eine Cloudsoftware Vorteile gegenüber einer lokal gehosteten Software bieten. Mindestens genauso schnell wie technologische Neuheiten auf den Markt kommen, ändert sich die Gefahrenlandschaft. Doch nur wenige Pharmahersteller haben entsprechende Ressourcen und dadurch das nötige Fachwissen, um ein umfassendes Cybersicherheitsprogramm zu entwickeln, umzusetzen und aufrechtzuerhalten. Mit einem cloudbasierten System können Hersteller die Cybersecurity-Expertise des Cloud Service Providers (CSP) nutzen. In einem Software-as-a-Service-Modell (SaaS) übernimmt der CSP die Aufgabe, Sicherheitsprogramme für die Anwendung zu pflegen und die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten. Dazu gehören die Einhaltung aktueller Cybersicherheitsvorschriften und bewährter Verfahren, die Aktualisierung der Software, wenn neue Sicherheitsbedrohungen und Schwachstellen entdeckt werden, sowie die laufende Überwachung und Erkennung von Bedrohungen:

Die Vertraulichkeit der Daten wird durch strenge Sicherheitsmaßnahmen wie Datenverschlüsselung, Firewalls, Benutzerauthentifizierung bis hin zur Zugriffskontrolle geschützt, um den Zugriff auf das System auf autorisierte Benutzer zu beschränken und Hacker daran zu hindern, sich Zugang zu unverschlüsselten Daten zu verschaffen. Die Datenintegrität wird durch Zugriffsbeschränkungen, die Implementierung digitaler Signaturen zur Verfolgung von Änderungen, die Verwendung von Datenvalidierungsmethoden zur Suche nach Anomalien und

Cloudlösungen, die nach den neuesten Standards konzipiert wurden, bieten zahlreiche Vorteile – insbesondere in Bezug auf Softwareupdates und Systemsicherheit. Bild: Communeer

Sie können auch einen SOC-2-Bericht anfordern, der eine Prüfung der Unternehmenskontrollen in Bezug auf Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz enthält.

Die Entwicklung einer sicheren Cloudlösung umfasst eine Reihe verschiedener Aspekte, darunter sichere Architektur, Backup und Notfallwiederherstellung, Überwachung der Sicherheit, Prüfung und Analyse sowie Incident Management. Dabei beginnt eine sichere Cloudanwendung mit sicheren Entwicklungsphasen. Ein DevSecOps-Ansatz, der die Cybersicherheit in jede Phase der Entwicklung und des Betriebs integriert, garantiert, dass bewährte Sicherheitspraktiken während des gesamten Software-Lebenszyklus angewandt werden, die es ermöglichen, Veränderungen in der Sicherheitsumgebung frühzeitig zu erkennen und darauf zu reagieren.

Sichere Architektur

Eine sichere Cloudarchitektur ist eine Kombination aus Sicherheitsmaßnahmen auf Daten-, Netzwerk- und Anwendungsebe-

die Überwachung ungewöhnlicher Verhaltensmuster gewährleistet. Die Datenverfügbarkeit wird in einer Cloudumgebung optimiert. Die Verfügbarkeit wird durch den Provider gesichert, und Daten sind abrufbar, selbst wenn die Einrichtungen oder Server des Nutzers nicht verfügbar sind. Georedundanz bietet zusätzlichen Schutz für kritische Anlagendaten.

Was bei der Providerwahl beachtet werden sollte

Um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten, sollten sichere Cloudanwendungen den aktuellen Best Practices entsprechen und alle Vorschriften zur Cybersicherheit in der Cloud einhalten. Die Verwaltung der Informationssicherheit wird durch ISO 27001 geregelt, die einen Rahmen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung von Sicherheitsmanagementsystemen, -verfahren und -richtlinien bietet. CSPs sollten ihre Sicherheitsprogramme in Übereinstimmung mit der ISO 27001 entwickeln. Sie sollten zudem über eine ISO-9001-Zertifizierung verfügen, die unter anderem Qualitätsmanagementsysteme für Softwareentwicklung und Cloudbereitstellung regelt.

Mit jedem Update einer SaaS-Lösung werden neue Module verfügbar, sodass Anwender in der Prozessindustrie vom aktuellen technologischen Stand profitieren. Bild: metamorworks/iStock

ne, um den Zugriff zu kontrollieren und Daten sowohl bei der Übertragung als auch der Speicherung zu schützen. Zu den Schlüsselelementen eines sicheren Entwurfs gehören die Identitäts- und Zugriffsverwaltung für autorisierte Benutzer, die Datenverschlüsselung für die Übertragung und Speicherung, Netzwerksicherheitsmaßnahmen wie Firewalls und Netzwerksegmentierung sowie Technologien zur Erkennung von Eindringlingen. So sollte beispielsweise HTTPS für die verschlüsselte Kommunikation zwischen dem Webbrowser und der Cloudanwendung verwendet und das System mit einer mandantenfähigen Architektur konzipiert werden, um die Daten der einzelnen Kunden zu isolieren.

Backup und Notfallwiederherstellung

Um eine kontinuierliche Datenverfügbarkeit zu gewährleisten, sollte der CSP über einen vollständig dokumentierten Backup- und Disaster-Recovery-Plan verfügen, der die Häufigkeit der Backups, die Standorte von Primär- und Backup-Servern, automatisierte Wiederherstellungsmethoden, Sicherheitsmaßnahmen für Backups und Wiederherstellungszeitziele festlegt. Georedundante Server und Datenbanksicherungen, bei denen Daten und Anwendungen an mehreren geografischen Standorten gespeichert werden, stellen sicher, dass die Daten auch dann noch verfügbar sind, wenn es in einem Rechenzentrum zu einem katastrophalen Verlust kommt oder die Daten aufgrund eines Serverproblems oder einer Naturkatastrophe vorübergehend nicht verfügbar sind. Die Daten sollten regelmäßig nach einem Zeitplan gesichert werden, der dem Unternehmen und der Art der gespeicherten Daten angemessen ist.

Überwachung der Sicherheit

Die Sicherheitsüberwachung für cloudbasierte Lösungen sollte sowohl eine externe als auch eine interne Überwachung umfassen. Die externe Überwachung von Bedrohungen umfasst das Durchsuchen der Bedrohungslandschaft auf Malware, neue Angriffsmethoden und Schwachstellen, welche die Anwendung selbst oder die mit ihr verbundenen Komponenten betreffen können. Die Bedrohungsanalyse kann eine Kombination aus automatisierten Methoden (zum Beispiel Honeypots) und manueller Überwachung von Informationen umfassen, die in Open- und Closed-Source-Sicherheitsforen verfügbar sind. Die interne Überwachung von Bedrohungen umfasst die automatisierte Überwachung von Netzwerk- und Systemsicherheit, deren Zustand, Verfügbarkeit und Leistung. Die Überwachung ermöglicht es den Anbietern, schnell zu reagieren, wenn ein Problem auftritt. Neben der Überwachung des Datenverkehrs sollte auch das Verhalten des Systems überwacht werden, um ungewöhnliche Verhaltensmuster zu erkennen, die auf einen Verstoß hindeuten könnten.

Von Prüfung bis Reaktionsplan

Das Testen und Analysieren von cloudbasierten Systemen ist ein wichtiger Aspekt, um die Sicherheit und Zuverlässigkeit des Systems zu gewährleisten. Die Infrastruktur und die gehosteten Anwendungen sollten regelmäßig getestet und analysiert werden, um Schwachstellen aufzuspüren und zu beseitigen. Dazu gehören neben automatisierten Tests externe Gray- und Blackbox-Penetrationstests und Bedrohungsmodellierung für die Software wie auch die Infrastruktur. Dieses Verfahren hilft bei der Ermittlung bisher unbekannter Schwachstellen und bei der Entwicklung von Softwarepatches oder anderen Abhilfemaßnahmen zur Stärkung des Systems.

Eine sichere Cloudanwendung muss über ein Incident Management und einen Reaktionsplan verfügen, um schnell auf Sicherheitsvorfälle reagieren zu können, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten beeinträchtigen. Dazu gehören Verfahren zur Erkennung und Meldung von Sicherheitsereignissen, zur Abschwächung ihrer Auswirkungen und zur Durchführung forensischer Analysen, um die Ursache und den Umfang des Vorfalls zu ermitteln. Mit einem gut definierten Plan für das Management von Sicherheitsvorfällen und die Reaktion darauf können CSPs schnell den Schaden eindämmen und wiederherstellen.

Mit Blick auf verschiedenste Parameter und Randbedingungen, führt an einer Cloudsolution häufig kein Weg vorbei. In Zukunft ist damit zu rechnen, dass Cloud Computing einen großen Zuwachs verzeichnen wird, angetrieben durch IIoT. Dabei sind aktuelle Standards für die Sicherheit der Softwareinfrastruktur fundamental.

Standards für ein Maximum an Sicherheit

SaaS-Anbieter sollten ihre Lösungen nach den neuesten Standards für Cybersicherheit entwickeln. Für Pharmahersteller, die ein SaaS-Angebot nutzen möchten, sollte standardgemäß das Zertifikat ISO 27001 vorliegen. Die internationale Norm für Informationssicherheitsmanagement zeigt, dass der Anbieter aktuelle Rahmenbedingungen bei der Cloudbereitstellung, Wartung und kontinuierlichen Verbesserung hinsichtlich der Sicherheit einhält. Insbesondere bei der Bewertung einer Plant-Process-Management-Software hinsichtlich ihrer Sicherheit ist eine ISO-27001-Zertifizierung ein guter Anhaltspunkt. Dabei prüft eine unabhängige Zertifizierungsstelle gründlich die Vorgehensweise des Providers und bewertet diese. Ergänzend zeigt die ISO-9001-Zertifizierung, dass die Qualitätsmanagementsysteme des Anbieters den heutigen Anforderungen entsprechen.

In den USA ist ein SOC-2-Bericht hilfreich. SOC 2 ist eine Art Audit, das Sicherheit, Verfügbarkeit und Integrität von Daten prüft. Wenn Plant Process Management in die Cloud verlagert wird, ist die Daten und Softwaresicherheit von entscheidender Bedeutung. Durch die Implementierung der richtigen Sicherheitsmaßnahmen bietet eine cloudbasierte PPM-Lösung Pharmaunternehmen eine hervorragende Basis, damit sie ihre Prozesse effektiv verwalten und sensible Daten schützen können. ■